WHAT IS CLAIMED IS:

1. An IC card supplied with an operating voltage by an electrical connection between each of external terminals and a read/write device, and including an input-output operation of data with an encoding process or a decoding process,

wherein a first processing operation is included in the encoding process or decoding process to uniformalize timings provided to operate an internal circuit and an operating current thereof.

2. The IC card according to claim 2, wherein the encoding process or decoding process includes an exponential residue multiplying operation applicable to RSA cryptography or the like.

3. The IC card according to claim 1, wherein the exponential residue multiplying operation is carried out by an encoding processing computing unit operated in response to instructions given from a central processing unit.

4. The IC card according to claim 3, wherein the encoding processing computing unit alternately computes $A = A^2 \mathrm{modN}$ and $A = \mathrm{ABmodN}$ with $A = 1$ and $B = X$ in response to X, Y and N inputted thereto, and allows a storage circuit to capture the computational result of $A^2 \mathrm{modN}$ as

valid data if a bit is logical 0 as viewed bit by bit from a high order of Y upon such a computation, and allows a storage circuit to capture the computational results of A^2 modN and ABmodN as valid data if the bit is a logical 1, and when the bit is given as the logical 0, the operation of computing A = ABmodN is set as the first processing operation.

5. The IC card according to claim 4, wherein said storage circuit is a register block comprising a read/write buffer and a plurality of registers in which the input/output of data is done through the read/write buffer, and

said computational result controls a gate circuit according to a logical 1 or 0 of a specific bit e_i of the Y, and controls the transmission of a write strobe signal supplied to a predetermined register, thereby allowing the predetermined register to store only valid data through the read/write buffer.

6. The IC card according to claim 4, wherein said storage circuit is a register block comprising a read/write buffer and a plurality of registers each of which performs the input/output of data through the read/write buffer, and

said computational result controls a gate circuit according to a logical 1 or 0 of a specific bit e_i of the

Y, and controls the transmission of a write strobe signal supplied to the read/write buffer, thereby allowing the predetermined register to store only valid data through the read/write buffer.

7. The IC card according to claim 4, wherein said storage circuit is a register block comprising a read/write buffer, a plurality of registers each of which performs the input/output of data through the read/write buffer, and a disturbance register, and

said computation result controls a selector provided between said read/write buffer and said disturbance register and plural registers according to a logical 1 or 0 of a specific bit e_i of the Y, thereby allowing a predetermined register to store valid data of the computational result written into the read/write buffer and allowing the disturbance register to store invalid data.

8. The IC card according to claim 3, wherein said encoding processing computing unit alternately computes A = A^2 modN and A = ABmodN with A = 1 and B = X in response to X, Y and N inputted thereto, and allows a storage circuit to capture the computational result of A^2 modN as valid data with its output timing if a bit is logical 0 as viewed bit by bit from a high order of Y upon such a computation, and allows a storage circuit to capture the

computational results of A^2 modN and ABmodN as valid data with its output timing if the bit is a logical 1, and said encoding processing computing unit continues the operation of A = A^2 modN even during a period from the output of the computational result of A = A^2 modN to the commencement of the computation of A = ABmodN, and continue the operation of A = ABmodN even during a period from the output of the computational result of A = ABmodN to the commencement of the computation of A^2 modN corresponding to the next bit inclusive of a change determining process of each bit of the Y.

9. The IC card according to claim 3, wherein said encoding processing computing unit computes and overflow-computes A = A^2 modN and A = ABmodN with A = 1 and B = X in response to X, Y and N inputted thereto, and allows a storage circuit to capture the computational result of A^2 modN as valid data if a bit is logical 0 as viewed bit by bit from a high order of Y upon such computations, and allows a storage circuit to capture the computational results of A^2 modN and ABmodN as valid data if the bit is a logical 1, and a computing operation of A = ABmodN at the logical 0 and an overflow computation unnecessary for each computing operation are defined as the first processing operations.

10. An IC card which is supplied with an operating

voltage by an electrical connection between each of external terminals and a read/write device, and which performs the input/output of data with an encoding process or a decoding process,

wherein said encoding process or said decoding process includes a first computation to allow timings provided to operate an internal circuit and an operating current thereof to have irregularities.

11. An IC card which is supplied with an operating voltage by an electrical connection between each of external terminals and a read/write device, and which performs the input/output of data with an encoding process or a decoding process,

wherein first cycles are included in intervals for respective computations in the encoding process or decoding process to allow timings provided to operate an internal circuit and an operating current thereof to have irregularities.

12. A microcomputer having a module configuration including an input-output operation of data with an encoding process or a decoding process,

wherein said encoding process or said decoding process includes a first processing operation to uniformalize timings provided to operate an internal circuit and an operating current thereof.

13. The microcomputer according to claim 12, wherein said module configuration is formed on one semiconductor substrate for the implementation thereof.

14. The microcomputer according to claim 13, wherein said encoding process or decoding process includes an exponential residue multiplying operation applicable to RSA cryptography or the like, and

said exponential residue multiplying operation is executed by an encoding processing computing unit operated in response to instructions given from a central processing unit.

15. The microcomputer according to claim 14, wherein said encoding processing computing unit alternately computes $A = A^2$ modN and A = ABmodN with A = 1 and B = X in response to X, Y and N inputted thereto, and allows a storage circuit to capture the computational result of A^2 modN as valid data if a bit is logical 0 as viewed bit by bit from a high order of Y upon such a computation, and allows a storage circuit to capture the computational results of A^2 modN and ABmodN as valid data if the bit is a logical 1, and when the bit is given as the logical 0, the operation of computing A = ABmodN is set as the first processing operation.

16. The microcomputer according to claim 14, wherein said encoding processing computing unit alternately computes $A = A^2$ modN and $A =$ ABmodN with $A = 1$ and $B = X$ in response to X, Y and N inputted thereto, and allows a storage circuit to capture the computational result of A^2 modN as valid data with its output timing if a bit is logical 0 as viewed bit by bit from a high order of Y upon such a computation, and allows a storage circuit to capture the computational results of A^2 modN and ABmodN as valid data with its output timing if the bit is a logical 1, and said encoding processing computing unit continues the operation of $A = A^2$ modN even during a period from the output of the computational result of $A = A^2$ modN to the commencement of the computation of $A =$ ABmodN, and continue the operation of $A =$ ABmodN even during a period from the output of the computational result of $A =$ ABmodN to the commencement of the computation of A^2 modN corresponding to the next bit inclusive of a change determining process of each bit of the Y.

17. The microcomputer according to claim 14, wherein said encoding processing computing unit computes and overflow-computes $A = A^2$ modN and $A =$ ABmodN with $A = 1$ and $B = X$ in response to X, Y and N inputted thereto, and allows a storage circuit to capture the computational result of A^2 modN as valid data if a bit is logical 0 as

viewed bit by bit from a high order of Y upon such computations, and allows a storage circuit to capture the computational results of A^2 modN and ABmodN as valid data if the bit is a logical 1, and a computing operation of A = ABmodN at the logical 0 and an overflow computation unnecessary for each computing operation are defined as the first processing operations.

18. The IC card according to claim 3, wherein said encoding processing computing unit computes $A = A^2R^{-1}$modN and $A = ABR^{-1}$modN according to the value of each bit of Y with A = 1 and B = X in response to X, Y and N inputted thereto, and

performs a normal operation for performing the subtraction W - N of N from the computational result W when an overflow occurs in each computational result, and a first operation for generating invalid data, based on a computation corresponding to the subtraction W - N even when no overflow occurs in each individual computational results, thereby outputting valid data according to the presence or absence of the overflow.

19. The IC card according to claim 18, wherein the computational result W of A^2R^{-1}modN or ABR^{-1}modN is stored in a first storage circuit,

the presence or absence of an overflow flag OV of an arithmetic unit is stored, the subtraction W - N of N from the computational result W stored in the first storage circuit is carried out after the residue multiplication, and when the overflow flag OV exits, the result of computation thereof is stored in the first storage circuit, whereas when the overflow flag OV is absent, the result of computation thereof is written in a second storage circuit different from the first storage circuit as the disturbance-aimed operation, and

the computational result of the first storage circuit is outputted as valid data.

20. The IC card according to claim 18, wherein the computational result W of A^2R^{-1}modN or ABR^{-1}modN is stored in a first storage circuit,

the presence or absence of an overflow flag OV of an arithmetic unit is stored, and

the subtraction W - N of N from the computational result W stored in the first storage circuit is carried out after the residue multiplication, and the computational result W - N is selected by a selector when the overflow flag OV exists, whereas when the overflow flag OV is absent, the computational result W of the first storage circuit is selected by the selector and stored in a second storage circuit, and said computational result W is outputted as valid data.

21. The IC card according to claim 18, wherein the computational result W of $A^{2}R^{-1}$modN or ABR^{-1}modN is stored in a first storage circuit,

the presence or absence of an overflow flag OV of an arithmetic unit is stored,

the subtraction W - N of N from the computational result W stored in the first storage circuit is carried out after the residue multiplication, and when the overflow flag OV exists, the subtraction W - N is stored in a second storage circuit, and when the overflow flag OV is absent, the subtraction W - N is stored in a third storage circuit,

when the overflow flag OV exists, the data stored in the second storage circuit is outputted as valid data, and

when the overflow flag OV is absent, the data stored in the first storage circuit is outputted as valid data.

22. The IC card according to claim 18, wherein the computational result W of $A^{2}R^{-1}$modN or ABR^{-1}modN is stored in a first storage circuit,

the presence or absence of an overflow flag OV of an arithmetic unit is stored, and

the subtraction W - N of N from the computational result W stored in the first storage circuit is stored in a second storage circuit after the residue multiplication, and when no overflow flag OV exists, the least significant addresses for selecting the first storage circuit and the second storage circuit are reversed and the first storage circuit is selected according to the address for selecting the second storage circuit to output the computational result as valid data, and when the overflow flag OV exists, the least significant addresses for selecting the first storage circuit and the second storage circuit are held as they are and the computational result of the second storage circuit is outputted as valid data.

23. The IC card according to claim 18, wherein the computational result W of A^2R^{-1}modN or ABR^{-1}modN is stored in a first storage circuit,

the presence or absence of an overflow flag OV of an arithmetic unit is stored, and

addresses for the first storage circuit and the second storage circuit are exchanged after the residue multiplication, the subtraction W - N of N from a computational result W selected according to an address for selecting the second storage circuit is performed, and the subtraction result W - N is stored in the second storage circuit selected according to an address for selecting the first storage circuit, and only when the overflow flag OV exists, the addresses are exchanged again and data stored in the first or second storage circuit selected according to the address for selecting the second storage circuit is outputted as valid data.

24. The IC card according to claim 18, wherein the computational result W of A^2R^{-1}modN or ABR^{-1}modN is stored in a first storage circuit,

the subtraction W - N of N from the computational result W of the first storage circuit is carried out after the residue multiplication and stored in a second storage circuit,

a borrow flag BR of an arithmetic unit at the subtraction of W - N is stored, and when the borrow flag BR exists, the least significant addresses for selecting the first storage circuit and the second storage circuit are reversed and the computational result W of the first storage circuit is outputted according to an address for selecting the second storage circuit,

when the borrow flag BR is absent, the least significant addresses for selecting the first storage circuit and the second storage circuit are held as they are and the computational result W - N of the second storage circuit is outputted according to the address for selecting the second storage circuit.

25. The microcomputer according to 14, wherein said encoding processing computing unit computes A = A^2R^{-1}modN and A = ABR^{-1}modN according to the value of each bit of Y

with A = 1 and B = X in response to X, Y and N inputted thereto, and

further performs a normal operation for performing the subtraction W - N of N from the computational result W when an overflow occurs in each computational result, and a first operation for generating invalid data, based on a computation corresponding to the subtraction W - N even when the overflow does not occur in each individual computational results,

whereby valid data is outputted according to the presence or absence of the overflow.

26. The microcomputer according to claim 25, wherein the computational result W of $A^{2}R^{-1}$modN or ABR^{-1}modN is stored in a first storage circuit,

the presence or absence of an overflow flag OV from an arithmetic unit is stored,

the subtraction W - N of N from the computational result W stored in the first storage circuit is carried out after the residue multiplication, and the result of computation thereof is stored in the first storage circuit when the overflow flag OV exists, whereas when the overflow flag OV is absent, the result of computation thereof is written into a second storage circuit different from the first storage circuit as the first operation, and

the computational result of the first storage circuit is outputted as valid data.

27. The microcomputer according to claim 25, wherein the computational result W of A^2R^{-1}modN or ABR^{-1}modN is stored in a first storage circuit,

the presence or absence of an overflow flag OV of an arithmetic unit is stored,

the subtraction W - N of N from the computational result W stored in the first storage circuit is carried out after the residue multiplication, and the computational result W - N is selected by a selector when the overflow flag OV exists, whereas when the overflow flag OV is absent, the computational result W of the first storage circuit is selected by the selector and stored in a second storage circuit, which in turn is outputted as valid data.

28. The microcomputer according to claim 25, wherein the computational result W of A^2R^{-1}modN or ABR^{-1}modN is stored in a first storage circuit,

the presence or absence of an overflow flag OV of an arithmetic unit is stored,

the subtraction W - N of N from the computational result W stored in the first storage circuit is carried out after the residue multiplication, and when the overflow flag OV exists, the subtraction result W - N is stored in a second storage circuit, whereas when the overflow flag OV is absent, the subtraction result W - N is stored in a third storage circuit,

when the overflow flag OV exists, the data stored in the second storage circuit is outputted as valid data, and

when the overflow flag OV is absent, the data stored in the first storage circuit is outputted as valid data.

29. The microcomputer according to claim 25, wherein the computational result W of A^2R^{-1}modN or ABR^{-1}modN is stored in a first storage circuit,

the presence or absence of an overflow flag OV of an arithmetic unit is stored, and

the subtraction result W - N of N from the computational result W stored in the first storage circuit is stored in a second storage circuit after the residue multiplication, and when the overflow flag OV is absent, the least significant addresses for selecting the first storage circuit and the second storage circuit are reversed and the first storage circuit is selected according to the address for selecting the second storage circuit to output the computational result as valid data, whereas when the overflow flag OV exists, the least significant addresses for selecting the first storage circuit and the second storage circuit are held as they are and the computational result of the second storage circuit is outputted as valid data.

30. The microcomputer according to claim 25, wherein the computational result W of A^2R^{-1}modN or ABR^{-1}modN is stored in a first storage circuit,

the presence or absence of an overflow flag OV of an arithmetic unit is stored,

addresses for the first storage circuit and the second storage circuit are exchanged after the residue multiplication, the subtraction W - N of N from a computational result W selected according to an address for selecting the second storage circuit is performed and the subtraction result W - N is stored in the second storage circuit selected according to an address for selecting the first storage circuit, and only when the overflow flag OV exists, the addresses are exchanged again and data stored in the first or second storage circuit selected according to the address for selecting the second storage circuit is outputted as valid data.

31. The microcomputer according to claim 5, wherein the computational result W of A^2R^{-1}modN or ABR^{-1}modN is stored in a first storage circuit,

the subtraction W - N of N from the computational result W of the first storage circuit is carried out after the residue multiplication and stored in a second storage circuit, a borrow flag BR is stored from an arithmetic unit at the subtraction of W - N, and when the borrow flag BR exists, the least significant addresses for selecting the first storage circuit and the second storage circuit are reversed and the computational result W of the first storage circuit is outputted according to an address for selecting the second storage circuit, and

when the borrow flag BR is absent, the least significant addresses for selecting the first storage circuit and the second storage circuit are held as they are and the computational result W - N of the second storage circuit is outputted according to the address for selecting the second storage circuit.